CPTO 11/5/04

1. A user information management apparatus constructed at at least one of (a) a server capable of making bidirectional communication with a user terminal, and (b) a user terminal, the apparatus comprising:

storage means for holding user information concerning a plurality of users who use the user terminal to be associated with a security level;

identification means for, when a user makes access to the server and an attempt is made by the user to use a predetermined application, identifying the user;

level determination means for, when the user makes access to the server, determining at which of a plurality of predetermined certification levels this access is;

transmission control means for enabling transmission of only the user information at the security level and the lower security level than said security level that corresponds to the determined level to the user terminal and/or another device among the user information held in the storage means; and

transmission disabling means for, following at least one of conditions (a) an elapse of a predetermined period of time and/or an execution of a predetermined operation after predetermined user information is enabled to be transmitted by transmission control means, and (b) an input a predetermined instruction from the user, disabling transmission of user information thus enabled to be transmitted.

2. A user information management apparatus according to claim 1, wherein said transmission disabling means enables only user information at a security level lower than the security level that corresponds to the determined level to be transmitted to the user terminal and/or another device.

3. A user information management apparatus according to claim 1 or claim 2, wherein said user identifying means uses at least one of (a) a password inputted by the user at the user terminal, (b) ID card information, (c) magnetic card information, (d) fingerprint, (e) voiceprint, and (f) iris print of the user which are read by the user terminal.

4. A user information management apparatus according to any one of claims 1 through 3, wherein said level determining means determines a predetermined technique employed by the user for the purpose of user identification, thereby determining a level.

5. (Amended) A user information management apparatus according to claim 1, wherein said user identifying means determines said user based on a predetermined instruction from an input device operated by said user at said user terminal, and said level determining means determines that the certification level is the lowest.

6. (Amended) A user information management apparatus according to claim 1, wherein, if a current certification level of the user is lower than a desired certification level required for data acquisition, said transmission control means instructs the user to take action required to level up to the required certification level.

7. (Amended) A user information management apparatus according to claim 1, wherein said transmission control means has means for defining a security level specific to said user information and means for managing said user information for said each security level.

8. (Amended) A user information management apparatus according to claim 1, wherein the apparatus is arranged to hold, in the storage means, information common to a plurality of users who use the user terminals as group data to be associated with a security level.

9. (Amended) A user information management apparatus according to claim 1, wherein, for a set of requested data, an index as an ID is obtained from a distance between a probability of such an event and data, and then, the obtained value is used to reconfirm a security.

10. (Amended) A user information management apparatus according to claim 1 wherein the apparatus is arranged so that said plurality of user terminals are classified in advance into a plurality of security divisions, and security division determining means is provided, thereby applying access restriction for such each security division of the user terminal that has made access.

11. A user information management apparatus according to claim 10, wherein the apparatus is arranged to determine the security division of the user terminal based on the registered number of users of the user terminal.

12. A user information management apparatus according to claim 10, wherein the apparatus is arranged so that, when the security division falls into a predetermined division

among said security divisions, and a certification level is lowered, data transmitted from the server to the user terminal is deleted before the certification level is changed to be lowered.

13. A user information management apparatus according to claim 10, wherein the apparatus is arranged so that, when the security division falls into a predetermined division among said security divisions, data inputted from the user terminal is automatically and/or periodically transmitted to a predetermined work area of the server.

14. (Amended) A user information management apparatus according to claim 1, wherein said transmission control means further comprises a user information use criterion storing means for storing a user information use criterion for a data requester in advance and a user information providing condition storing means for storing a user information providing condition for a data provider in advance, and, when the user information use criterion and the user information providing condition are compared with each other, and transmission is controlled based on the comparison result, if user information other than that on a user determined by the user determination means is contained in data, the user information providing condition of the user is obtained, and comparison with the user information use criterion is carried out, thereby determining whether or not transmission is carried out.

15. A user information management method in the user information management apparatus constructed at at least one of (a) a server capable of making bidirectional communication with a user terminal and (b) the user terminal, the method comprising the steps of:

storage step of holding user information concerning a plurality of users who use the user terminal to be associated with a security level;

identification step of, when a user makes access to the server and an attempt is made by the user to use a predetermined application, identifying the user;

level determining step of, when the user makes access to the server, determining at which of a plurality of predetermined certification levels this access is;

transmission control step of enabling transmission of only the user information at the security level and the lower security level than said security level that corresponds to the determined level to the user terminal and/or another device among the user information held in the storage step; and

transmission disabling step of, following at least one of conditions (a)an elapse of a predetermined period of time and/or an execution of a predetermined operation after predetermined user information is enabled to be transmitted by transmission control step, and (b) an input of a predetermined instruction from the user, disabling transmission of user information thus enabled to be transmitted.

16. A user information management method according to claim 15, wherein said transmission disabling step enables only user information at a security level lower than the security level that corresponds to the determined level to be transmitted to the user terminal and/or another device.

17. A user information management method according to claim 15 or claim 16, wherein said user identifying step uses at least one of (a) a password inputted by the user at the user terminal, (b) ID card information, (c) magnetic card information, (d) fingerprint, (d) voiceprint, and (e) iris print of the user which are read by the user terminal.

18. (Amended) A user information management method according to claim 15, wherein said level determining step determines a predetermined technique employed by the user for the purpose of user identification, thereby determining a level.

19. (Amended) A user information management method according to claim 15, wherein said user identifying step determines said user based on a predetermined instruction from an input device operated by said user at said user terminal, and, in this case, said level determining step determines that the certification level is the lowest.

20. (Amended) A user information management method according to claim 15, wherein, if a current certification level of the user is lower than a desired certification level required for data acquisition, said transmission control step instructs the user to take action required to level up to the required certification level.

21. (Amended) A user information management method according to claim 15, wherein said transmission control step has the step of defining a security level specific to said user information and the step of managing said user information for said each security level.

22. (Amended) A user information management method according to claim 15, wherein the method is arranged to hold, in the storage step, information common to a plurality of users who use the user terminals as group data to be associated with a security level.

23. (Amended) A user information management method according to claim 15, wherein the method comprises the step of obtaining, for a set of requested data, an index as an ID from a distance between a probability of such an event and data, and then using the obtained value to reconfirm a security.

24. (Amended) A user information management method according to claim 15, wherein the method is arranged so that said plurality of user terminals are classified in advance into a plurality of security divisions, and security division determining step is provided, thereby applying access restriction for such each security division of the user terminal that has made access.

25. A user information management method according to claim 24, wherein the method is arranged to determine the security division of the user terminal based on the registered number of users of the user terminal.

26. A user information management method according to claim 24, wherein the method is arranged so that, when the security division falls into a predetermined division among said security divisions, and a certification level is lowered, data transmitted from the server to the user terminal is deleted before the certification level is changed to be lowered.

27. A user information management method according to claim 24, wherein the method is arranged so that, when the security division falls into a predetermined division among said security divisions, data inputted from the user terminal is automatically and/or periodically transmitted to a predetermined work area of the server.

28. (Amended) A user information management method according to claim 15, wherein, a user information use criterion for a data requester is stored in advance, and a user information providing condition for a data provider is stored in advance, and when the transmission control step further compares the user information use criterion and the user information providing condition with each other, so that transmission is controlled based on the comparison result, if user information other than that on a user determined by the user determination means is contained in data, the user information providing condition of the user is obtained, and comparison with the user information use criterion is carried out, thereby determining whether or not transmission is carried out.

29. A recording medium having recorded therein in a computer readable state a control program for executing the user information management method in the user information management apparatus constructed at at least one of (a) a server capable of making bidirectional communication with a user, and (b) the user terminal, the recording medium having recorded therein in a computer readable state a control program for executing the user information management method comprising the steps of:

storage step of holding user information concerning a plurality of users who use the user terminal to be associated with a security level;

identification step of, when a user makes access to the server and an attempt is made by the user to use a predetermined application, identifying the user;

level determining step of, when the user makes access to the server, determining at which of a plurality of predetermined certification levels this access is;

transmission control step of enabling transmission of only the user information at the security level and the lower security level than said security level that corresponds to the determined level to the user terminal and/or another device among the user information held in the storage step; and

transmission disabling step of, after elapse of a predetermined period of time and/or after execution of a predetermined operation after predetermined user information is enabled to be transmitted by transmission control step, or alternatively, according to a predetermined instruction from the user, disabling transmission of user information thus enabled to be transmitted.

30. A recording medium having recorded therein in a computer readable state a control program for executing the user information management method according to claim 29, wherein said transmission disabling step enables transmission of only user information at a security level lower than said security level corresponding to said determined level to said user terminal and/or another device.

31. A recording medium having recorded in a computer readable state a control program for executing the user information management method according to claim 29 or claim 30, wherein said user identifying step uses at least one of (a) a password inputted by the user at the user terminal , (b) any one or more of ID card information, (c) magnetic card information, (d) fingerprint, (e) voiceprint, and (f) iris print of the user.

32. (Amended) A recording medium having recorded in a computer readable state a control program for executing the user information management method according to claim 29, wherein said level determining step determines a predetermined technique employed by the user for the purpose of user identification, thereby determining a level.

33. (Amended) A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to claim 29, wherein said user identifying step determines said user based on a predetermined instruction from an input device operated by said user at said user terminal, and, in this case, said level determining step determines that the certification level is the lowest.

34. (Amended) A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to claim 29, wherein, if a current certification level of the user is lower than a desired certification level required for data acquisition, said transmission control step instructs the user to take action required to level up to the required certification level.

35. (Amended) A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to claim 29, wherein said transmission control step has the step of defining a security level specific to said user information and the step of managing said user information for said each security level.

36. (Amended) A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to claim 29, wherein the recording medium is arranged to hold, in the storage step, information common to a plurality of users who use the user terminals as group data to be associated with a security level.

37. (Amended) A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to claim 29, wherein the recording medium is arranged so that, for a set of requested data, an index as an ID is obtained from a distance between a probability of such an event and data, and then, the obtained value is used to reconfirm a security.

38. (Amended) A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to claim 29, wherein the recording medium is arranged so that said plurality of user terminals are classified in advance into a plurality of security divisions, and security division determining step is provided, thereby applying access restriction for such each security division of the user terminal that has made access.

39. A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to claim 38, wherein the recording medium is arranged to determine the security division of the user terminal based on the registered number of users of the user terminal.

40. A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to claim 38, wherein the recording medium is arranged so that, when the security division falls into a predetermined division among said security divisions, and a certification level is changed to be lowered, data transmitted from the server to the user terminal is deleted before the certification level is lowered.

41. A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to claim 38, wherein, when the security division falls into a predetermined division among said security divisions, data inputted from the user terminal is automatically and/or periodically transmitted to a predetermined work area of the server.

42. (Amended) A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to claim 29, wherein the recording medium is arranged so that, a user information use criterion for a data requester is stored in advance, and a user information providing condition for a data provider is stored in advance, and when the user information use criterion and the user information providing condition are compared with each other, and transmission is controlled based on the comparison result, if user information other than that on a user determined by the user determination means is contained in data, the user information providing condition of the user is obtained, and comparison with the user information use criterion is carried out, thereby determining whether or not transmission is carried out.

43. A user information management apparatus comprising:

an access accepting section for accepting data access;

an access privilege determining section for determining the presence or absence of access privilege relevant to data on the access accepted at the access accepting section; and

an access management section for making a change in access privilege relevant to data on the access accepted at the access accepting section.

44. A user information management apparatus according to claim 43, wherein the access privilege determining section determines the presence or absence of access privilege based on an access privilege table in which data and access privilege are associated with each other.

45. A user information management apparatus according to claim 43, wherein the access privilege determining section determines the presence or absence of access privilege based on the access privilege described in data.

46. A user information management apparatus according to claim 43, wherein the access management section has an access privilege change information output means for outputting access privilege change information indicative of the changed access privilege.

47. A user information management apparatus according to claim 46, wherein the access privilege determining section has access privilege change information acquiring means for acquiring access privilege change information from the access privilege change information output means.

48. A user information management apparatus according to claim 46, wherein the access accepting section accepts an access from a device, and the access privilege change information output means transmits the access privilege change information to said device.

49. A user information management apparatus according to claim 43, further comprising an access privilege change condition acquiring section for acquiring a condition for changing access privilege.

50. A user information management apparatus according to any one of claims 43 to 47, wherein a change in access privilege at the access management section is a change in access level privilege within the range of data that can be accessed.

51. A user information management apparatus according to any one of claims 43 to 47, wherein the data to be accessed is classified by the owners, and a change in access privilege is a change in access privilege to data of another owner associated with the accessed data.

52. A user information management apparatus according to claim 51, wherein the access management section is restored to the original access privilege after the completion of processing by said access change.

53. A user information management apparatus according to any one of claims 43 to 47, wherein, when it is determined that an access at the access accepting section is provided without privilege at the access privilege determining section, there is further provided an certification acquiring section that requests acquisition of access privilege.

54. A user information management apparatus according to claim 49, wherein a condition for changing said access privilege is at least one of: (a) a no access continuation time, (b) data access count, (c) an instruction from an accessing person, (d) an instruction from an operating system, (e) an instruction from an application program, (f) an elapsed time after starting access, (g) time information, (h) access rejection count, (i) an elapsed time after changing access privilege, and (j) a combination of two or more thereof.

55. A user information management program causing a computer to execute the steps of:

access accepting step of accepting data access;

access privilege determining step of determining the presence or absence of access privilege to the access data accepted in the access accepting step; and

access management step of changing the access privilege relevant to data on the access accepted in the access accepting step.

56. A user information management program according to claim 55, the program causing a computer to execute the access privilege change information output step of outputting access privilege change information that is information indicative of the changed access privilege in the access management step.

57. A user information management program according to claim 55, the program causing a computer to execute the access privilege change condition acquiring step of acquiring a condition for changing access privilege.